Report di Laboratorio: Sfruttamento Vulnerabilità PostgreSQL

Accesso Iniziale e Privilege Escalation a Root

Josh Van Edward D. Abanico

21 gennaio 2026

Sommario

Il presente documento descrive le attività di Penetration Testing condotte sulla macchina target *Metasploitable 2*. L'attività si concentra sullo sfruttamento di una configurazione vulnerabile del servizio PostgreSQL per ottenere un accesso iniziale, seguito dall'elevazione della sessione a Meterpreter. Infine, viene eseguita un'analisi automatizzata delle vulnerabilità locali che porta con successo all'escalation dei privilegi, garantendo l'accesso amministrativo (root) al sistema.

Indice

1 Obiettivo dell'Esercitazione

L'obiettivo è simulare un ciclo di attacco mirato sfruttando il framework **Metasploit**. Gli step operativi comprendono:

1. Sfruttamento del servizio PostgreSQL per ottenere una shell remota.
2. Upgrade della connessione a sessione Meterpreter.
3. Analisi delle vulnerabilità locali tramite moduli di ricognizione.
4. Esecuzione di un exploit locale per ottenere i privilegi di `root`.

2 Fase 1: Accesso Iniziale (Exploitation)

È stato identificato il servizio PostgreSQL attivo sulla porta standard 5432. Per sfruttare la vulnerabilità, è stato selezionato il modulo exploit dedicato che permette l'upload di un payload dinamico.

Modulo utilizzato: `exploit/linux/postgres/postgres_payload`

Di seguito la configurazione dei parametri di rete (RHOSTS per il target e LHOST per la macchina attaccante):

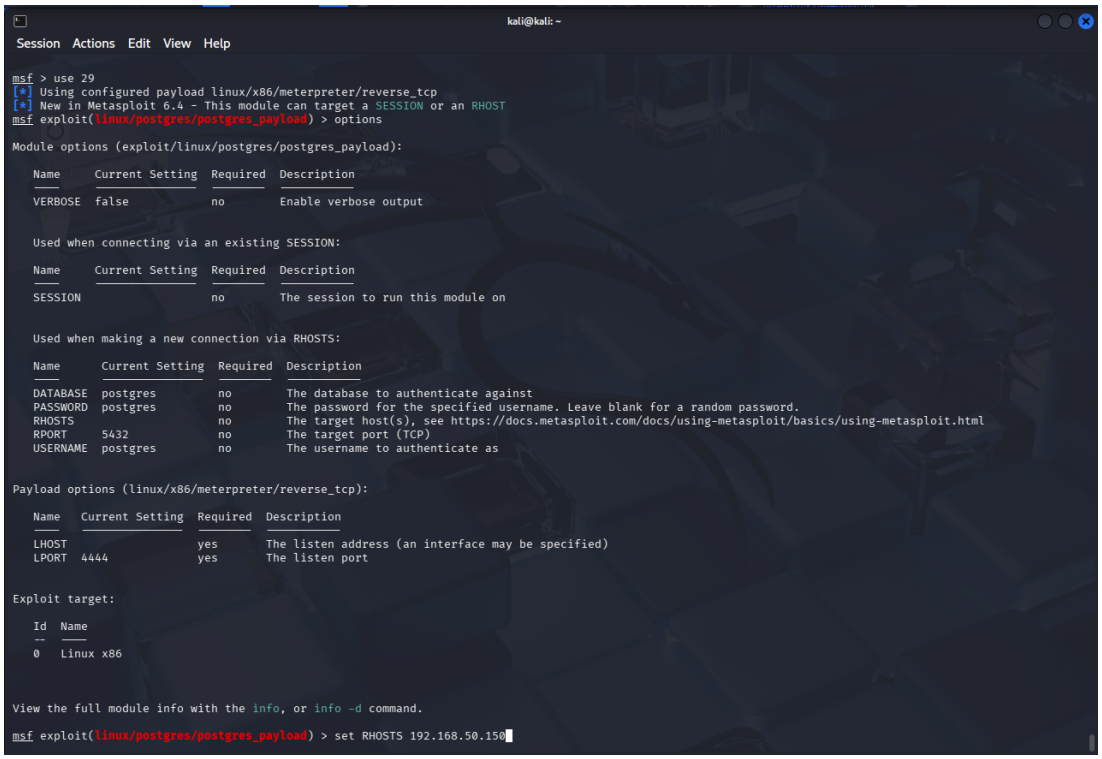

Figura 1: Selezione del modulo exploit e configurazione RHOSTS.

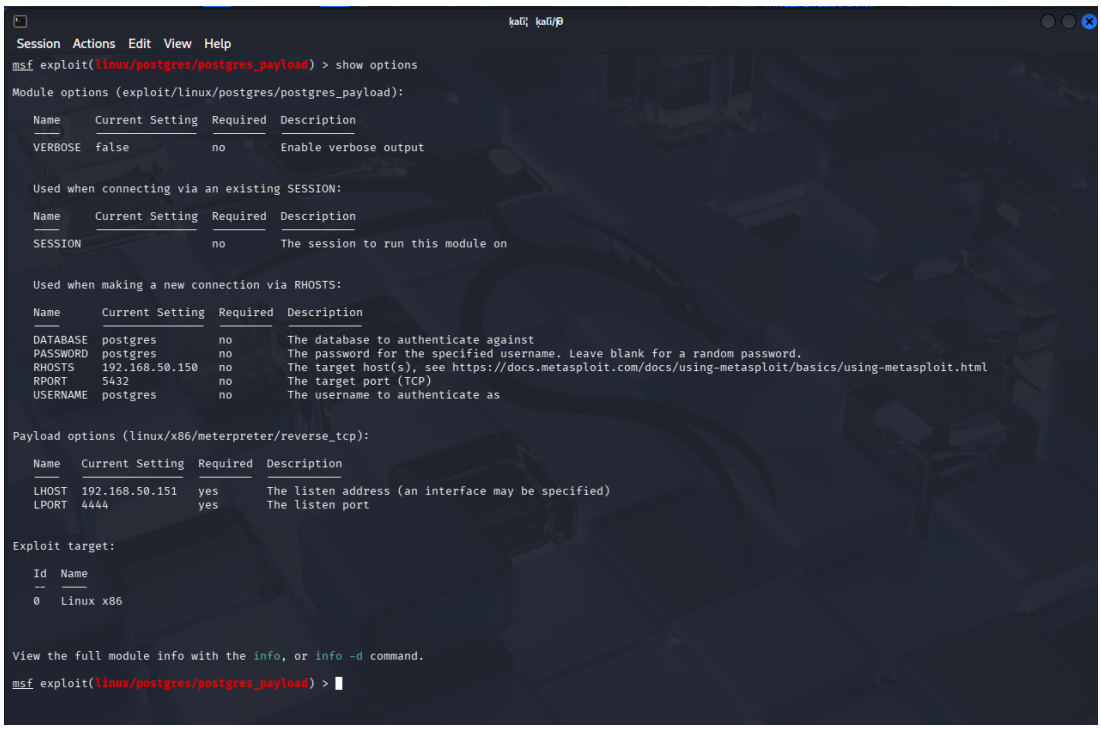

Figura 2: Verifica delle opzioni (Show Options) prima dell'esecuzione.

L'attacco è stato lanciato con successo, aprendo una sessione Meterpreter. Il comando `getuid` conferma che stiamo operando con l'utente di servizio `postgres`.

Figura 3: Esecuzione exploit riuscita e verifica utente (postgres).

3 Fase 2: Post-Exploitation e Reconnaissance

Ottenuto l'accesso iniziale, la sessione è stata messa in background per utilizzare moduli di ricognizione post-exploitation. L'obiettivo è identificare vettori per ottenere i privilegi di `root`.

Modulo utilizzato: `post/multi/recon/local_exploit_suggester`

Il modulo analizza la versione del kernel e i pacchetti installati per suggerire exploit locali applicabili.

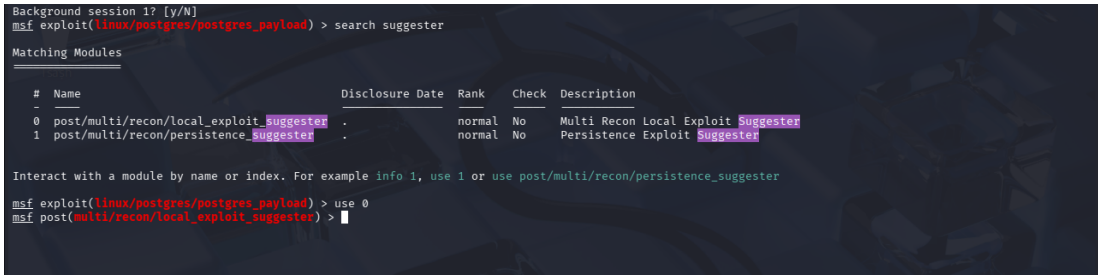

Figura 4: Ricerca del modulo Local Exploit Suggester.

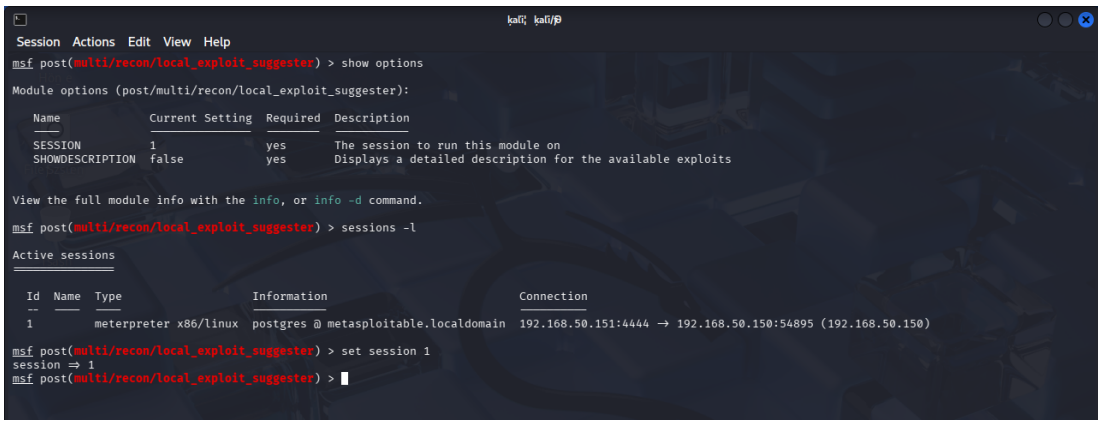

Figura 5: Configurazione del suggester sulla Sessione 1.

L'output del modulo ha evidenziato diverse vulnerabilità critiche nel kernel Linux target, come mostrato di seguito:

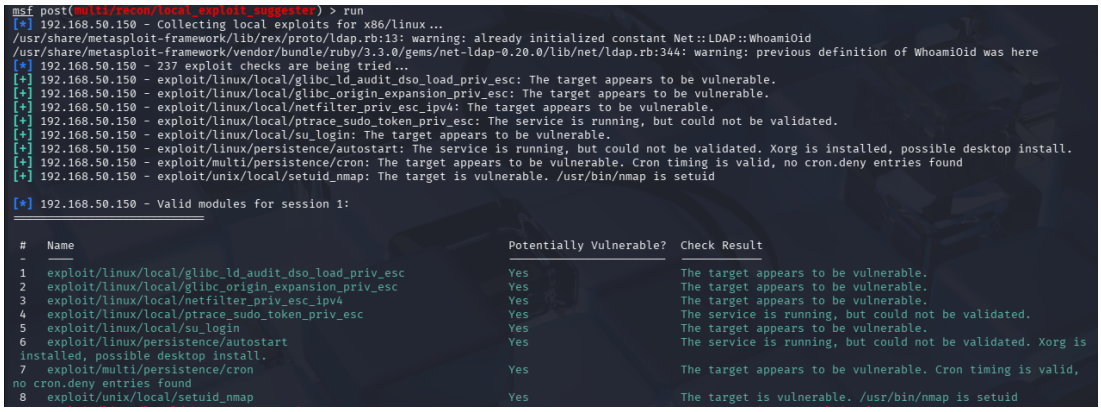

Figura 6: Risultati del Suggester: vulnerabilità rilevate (es. glibc, netfilter).

4 Fase 3: Privilege Escalation

Tra le vulnerabilità rilevate, è stato selezionato l'exploit relativo alla libreria **glibc** (`glibc_ld_audit_dso_lo`

Durante la configurazione, è stato necessario modificare la porta locale (`LPORT 3456`) per evitare conflitti con la sessione precedente. L'esecuzione dell'exploit ha avuto successo, aprendo una nuova sessione Meterpreter.

Come evidenziato dallo screenshot seguente, il comando `getuid` conferma l'avvenuta escalation dei privilegi: **Server username: root**.

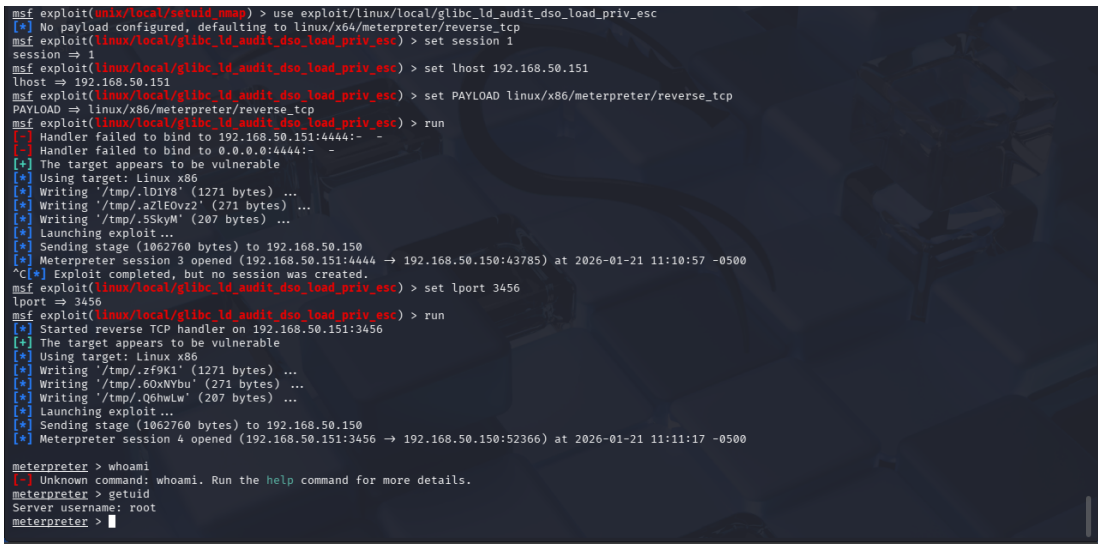

Figura 7: Esecuzione exploit glibc e conferma privilegi Root.

5 Conclusioni

L'attività di laboratorio ha dimostrato con successo la catena di attacco completa. Partendo da un servizio mal configurato (PostgreSQL), è stato possibile ottenere un accesso iniziale limitato.

Successivamente, l'uso di strumenti di ricognizione automatizzata (*Local Exploit Suggester*) è risultato fondamentale per identificare rapidamente vulnerabilità critiche nel kernel. L'applicazione dell'exploit suggerito ha permesso di elevare i privilegi fino al livello massimo (`root`), garantendo il controllo totale del sistema target e dimostrando l'importanza cruciale del patch management sia a livello applicativo che di sistema operativo.